4 文科高第 367 号
令和４年６月 22 日

各国立大学法人の長
大学及び高等専門学校を設置する各地方公共団体の長
各公立大学法人の理事長
大学及び高等専門学校を設置する各学校法人の理事長
放送大学学園理事長
大学を設置する各学校設置会社の代表取締役
各大学共同利用機関法人機構長
独立行政法人国立高等専門学校機構理事長
殿

文部科学省総合教育政策局長
藤原章夫

文部科学省高等教育局長
増子宏

文部科学省研究振興局長
池田貴城

大学等におけるサイバーセキュリティ対策等の継続的な取り組みについて（通知）

大学等におけるサイバーセキュリティ対策等については、令和元年に発出した「大学等におけるサイバーセキュリティ対策等の強化について（通知）」（令和元年５月 24 日付元文科高第 59 号）に基づき、各大学等において対応いただいているところです。

昨年度、文部科学省が大学等から報告を受けたインシデントは、メール誤送信や情報の意図せぬ公開など、基本的な情報セキュリティ対策の未実施や意識の欠如に起因するものが半数近く発生しており、人為的なミス、抜け漏れのない組織をどのように構築・維持していくのか、が課題となっています。また、標的型攻撃（高度サイバー攻撃）に象徴されるマルウェア感染や不正アクセス等のサイバー攻撃についても、一時は減少傾向にあったものの活発化しつつあります。

上記通知においても大学等に対して設置種別ごとに取り組むべき事項を示し、特に国立大学等に対してはフォローアップ等調査を実施して取り組み状況を把握していますが、取り組みに比して事案等が急速に減少するわけでもなく、引き続き地道な継続的な取り組みが必要と認識しています。

また、新技術の進展や新たな脅威の登場により対応しなければいけない内容は増加する一方であるものの、守るべきものは保有する情報資産であり、各大学等でリスク評価を踏まえて真に守るべき情報資産と認定したものであります。特に、先端的な技術情報については大学等のみならず産学官連携等で産業界と情報共有をする機会も日常的に行われているものと思慮され、企業等においては産業競争力強化法に基づく技術情報等の管理がなされているところ、それを共

有する大学等においてもサプライチェーンという観点から、同様の管理が求められる機会も多くなると想定されるところです。

さらに、令和３年９月 28 日に閣議決定された「サイバーセキュリティ戦略」においても、「経済社会基盤を支える各主体における取組③（大学・教育研究機関等）」として先端的な技術情報を保有する大学等だけではなく、大学等の保有する多岐にわたる情報資産を重要視し、すべての大学等において自律的な対策を講じることを求めています。

ついては、とりまとめの趣旨に基づき、国立大学法人等においては既存の「サイバーセキュリティ対策等基本計画」を別添の取組を踏まえて令和４年９月末までに改定願います。また、公私立の大学及び高等専門学校においては、別添の取組により、サイバーセキュリティ対策等の強化に努めていただくよう改めてお願いします。

○ 国立大学法人等･･･国立大学法人、大学共同利用機関法人、放送大学学園及び独立行政法人国立高等専門学校機構を指す。

○ 大学等･･･「国立大学法人等」に公立大学及び公立高等専門学校並びに私立大学等を設置する学校法人を加えたものを指す。

＜本件連絡先＞ 文部科学省代表番号：０３－５２５３－４１１１
（国立大学法人）高等教育局国立大学法人支援課法規係　内線：３７６０
（公立大学等）高等教育局大学振興課公立大学係　内線：３３７０
（私立大学等）高等教育局私学部私学行政課企画係　内線：２５３３
（放送大学学園）総合教育政策局生涯学習推進課放送大学振興係　内線：３４５９
（高等専門学校）高等教育局専門教育課高等専門学校係　内線：３３４７
（大学共同利用機関法人）研究振興局大学研究基盤整備課機構総括係　内線：４３０２
（その他サイバーセキュリティ等全般に関すること）大臣官房政策課サイバーセキュリティ・情報化推進室　情報統括係・サイバーセキュリティ係　内線：２２４８

別添

サイバーセキュリティ対策にかかる実施すべき事項

１．リスク管理体制の構築

（１）リスクへの対応認識と確認と体制の構築

①ポリシーや対策推進計画、管理規定の策定

②管理体制の構築

③リスク対策にかかる予算、資源

２．リスクの特定

（１）リスクの特定と評価

①大きなリスクの対象となりうる情報の確認

②大きなリスクの特定

③情報機器の洗い出し

３．リスク対策

（１）リスクへの対策

①守るべき情報の保護

②情報機器の脆弱性対応

③災害等などのリスク対策

④構成員へのセキュリティ意識の徹底

４．サプライチェーンリスクへの対応

（１）外注や共同研究、重要プロジェクトにかかるリスク管理

５．インシデント対応体制の構築

（１）インシデントの緊急体制と復旧体制の整備

６．セキュリティ運用の実施

（１）脅威動向や脆弱性情報取集、監視、侵入の特定などの運用について

７．監査等での運用チェック

（１）技術的、オペレーション等の監査について

１．リスク管理体制の構築

（１）リスクへの対応認識と確認と体制の構築

①ポリシーや対策推進計画、管理規定の策定

各機関において情報セキュリティ水準を適切に維持し、リスクを総合的に低減させるため、ポリシーをはじめとする管理文書を整備すること。

【例】

・情報セキュリティポリシーの策定
・ポリシーをもとにした情報セキュリティ対策基本計画を策定する。
・情報セキュリティを維持するための具体的な実施手順書を作成する。

【参考】

・政府機関等のサイバーセキュリティ対策のための統一基準群（NISC）
https://www.nisc.go.jp/policy/group/general/kijun.html
→統一基準群は、国の行政機関及び独立行政法人等の情報セキュリティ水準を向上させるための統一的な枠組みであり、国の行政機関及び独立行政法人等の情報セキュリティのベースラインや、より高い水準の情報セキュリティを確保するための対策事項が規定されている。「政府機関等のサイバーセキュリティ対策のための統一基準」や「政府機関等の対策基準策定のためのガイドライン」は情報セキュリティ確保のための基本的要件を示したものとなるため、参考とされたい。

・「高等教育機関向けサンプル規程集」（国立情報学研究所）
https://www.nii.ac.jp/service/sp/
→上記統一基準群に準拠して、実際の情報セキュリティ運用を想定したサンプル規定集である。各項目ごとに具体的なサンプル規定が解説付きで公開されている。

・その他各組織・団体が作成している最新のガイドラインや対策資料等

②管理体制の構築

サイバーセキュリティ対策を行うための管理体制を構築すること。

【例】

・CISO 以下、政府統一基準に準拠したサイバーセキュリティ管理体制の構築。

・司令塔機能を強化するため、外部からの専門人材の登用や担当部署を設置する。

【参考】

・サイバーセキュリティ経営ガイドライン　Ver 2.0（経済産業省・独立行政法人情報処理推進機構）

https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0.pdf

→以下箇所に、管理体制構築についての記載がある。

III. サイバーセキュリティ経営の重要１０項目

指示２ サイバーセキュリティリスク管理体制の構築

・サイバーセキュリティ体制構築・人材確保の手引き（第 1.1 版）（経済産業省）

https://www.meti.go.jp/press/2021/04/20210426002/20210426002-1.pdf

③リスク対策にかかる予算、資源

サイバーセキュリティ対策実施にかかる予算及び人材確保を継続的に措置する。

【例】

・機関内のリスク管理委員会等で情報セキュリティ対策に必要な予算や体制を検討し、経営決定の会議にて承認・措置する。

・機関内でサイバーセキュリティや情報システム部門の人材を確保するため、育成やキャリアパスを構築する。

【参考】

・サイバーセキュリティ経営ガイドライン　Ver 2.0（経済産業省・独立行政法人情報処理推進機構）
https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0.pdf
→以下箇所に、管理体制構築についての記載がある。
III. サイバーセキュリティ経営の重要１０項目
指示２ サイバーセキュリティリスク管理体制の構築

・サイバーセキュリティ体制構築・人材確保の手引き（第 1.1 版）（経済産業省）
https://www.meti.go.jp/press/2021/04/20210426002/20210426002-1.pdf

・CISO ハンドブック　NPO 日本ネットワークセキュリティ協会（JNSA）
https://www.jnsa.org/result/2018/act_ciso/

２．リスクの特定

（１）リスクの特定と評価

①大きなリスクの対象となりうる情報の確認

機関内で保有する情報について洗い出し、機密性の確認・整理を行う。また、法人文書ファイル管理簿にもその情報を付記する。

【例】

以下に該当する情報について特定し、機密性の確認・整理を行う。

・個人情報
・先端技術情報
・法令の定めにより管理すべき情報

【参考】

・リスクアセスメントの実施の手引き（NIST）
https://www.ipa.go.jp/files/000025325.pdf

・政府機関等のサイバーセキュリティ対策のための統一基準（令和３年度版）（NISC）
https://www.nisc.go.jp/pdf/policy/general/kijyunr3.pdf

②大きなリスクの特定

リスク対象となる情報について、漏えい・棄損した場合にどのような事態に陥るのか、リスク特定を行う。

【例】

・被害金額を算定しリスクを特定する。
・情報の価値を点数化することによりリスクを特定する。

【参考】

・リスクアセスメントの実施の手引き（NIST）
https://www.ipa.go.jp/files/000025325.pdf

・情報セキュリティポリシー策定におけるリスク評価の一事例（JST 計測と制御 第 57 巻 第 6 号 2018 年 6 月号）
https://www.jstage.jst.go.jp/article/sicejl/57/6/57_450/_pdf/-char/ja

③情報機器の洗い出し

機関内で保有・稼働している情報機器やサービスについて、管理対象を特定するために状況を把握する。

【例】

・自組織の名前で外部に公開している情報機器やサービス（外部ホスティングサービスやクラウド等を利用している場合を含む）を定期的に棚卸する。
・緊急時に停止可能な情報機器と業務継続のため無停止が求められる情報機器についても事前に把握しておく。
・グローバルＩＰアドレスを付与する情報機器やサービス（外部ホスティングサービスやクラウド等を利用している場合を含む）は漏れの無いよう定期的に棚卸をするなど管理を行う。
・グローバルＩＰアドレスを使用する情報機器については、通信要件を把握して不必要な接続を遮断する等適切なアクセス制御と権限管理を行う。研究室等において管理者に無許可でサーバ等が設置されないよう必要な措置等を講ずる。

【参考】

・「重要インフラのサイバーセキュリティを改善するためのフレームワーク」
（NIST・IPA）
https://www.ipa.go.jp/security/publications/nist/index.html

・効果的なサイバー防御のための CIS クリティカルセキュリティコントロール
（The Center for Internet Security）
https://www.cisecurity.org/wp-content/uploads/2017/03/CIS-CSC_v6.1_Japanese_Final_r1.pdf

３．リスク対策

（１）リスクへの対策

①守るべき情報の保護

リスク評価に応じて、適切な情報セキュリティ対策を講じること。

【例】

- 機密性２以上の情報資産を扱う可能性のあるシステムでは、多要素認証の導入や定期的なログの確認など、不正アクセス対策を強化する。
- 多要素認証を導入できない場合は、強度の高いパスワードの設定や、定期的なパスワード変更の実施、学外の他システムとのパスワードの使い回しの禁止など、対策を強化する。
- ユーザのアカウント情報は定期的に棚卸しを行うとともに、退職者のアカウントは速やかに削除又は停止する。
- 法人内に存在する機密性２以上の情報資産を扱うサーバ、特に ActiveDirectory 等の認証機能を有しているサーバを特定し、アカウントの棚卸し、ログ取得、パッチ適用等の基本的な対策を実施する。
- 先端技術情報など重要情報を扱う部門の ActiveDirectory 等認証機能を有するサーバ等については、標的型攻撃を踏まえた多層防御及び堅牢化を行う。
- 大学等支給端末において盗難、紛失、不正プログラムの感染等により情報が窃取されることを防止するための技術的な措置や、大学等支給以外の端末において不正プログラムの感染等により情報窃取されることを防止するための利用時の措置に関する手順等を整備する。
- USB メモリ等の外部電磁的記録媒体を用いて要機密情報を取り扱うことを許容する場合は、取扱いに関する手順等を定める。
- 教室、研究室、事務室、会議室、サーバ室等の情報を取り扱う区域において、区域の明示、施錠、入退室管理等の対策を講じ、当該区域で取り扱う情報や情報システム等のセキュリティを確保するとともに、重要な書類や外部記録媒体、ノートパソコン等の備品、その他毒物、劇物等の化学物質等を含む適正な管理が必要な物品等について、管理を徹底し、紛失・盗難の対策を講じる。
- テレワーク環境等の機関外での端末利用についても、リスク評価に応じて、適切な情報セキュリティ対策を講じる。
- クラウド上でのシステム構築、データの保存・管理が増加していることを前提とし、大学等の自組織内情報システムに加え、外部のサービスプロバイダーを利用するシステムやデータについてもデータ保護について検討を行う。

【参考】

・ログを活用した Active Directory に対する攻撃の検知と対策（JPCERT）
https://www.jpcert.or.jp/research/AD.html

・高度サイバー攻撃(APT)への備えと対応ガイド～企業や組織に薦める一連のプロセスについて（JPCERT）
https://www.jpcert.or.jp/research/apt-guide.html

・テレワークセキュリティガイドライン （総務省）
https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

・CIS Controls （Center for Internet Security）
https://learn.cisecurity.org/cis-controls-download

②情報機器の脆弱性対応

保有している情報機器の脆弱性について定期的に情報収集を行い、リスクに応じて脆弱性対応を適宜行うこと。

【例】

・構成管理ソフトウェアの導入による脆弱性情報の収集自動化、適応自動化

【参考】

・脆弱性対策の効果的な進め方 ツール活用編（IPA）
https://www.ipa.go.jp/topic/isec-technicalwatch-201902.html

③災害等などのリスク対策

各法人の災害復旧計画（DR）及び事業継続計画（BCP）について、情報セキュリティインシデントにかかる事案についても想定を含めること。

【例】

・サイバー攻撃やその他大規模システム障害等を踏まえた、可用性の維持に係るサイバーセキュリティ対策等の記載があるかどうか確認する。記載がない場合、各機関の実情を踏まえ、想定する事態が発生した場合に必要な事項を記載する。
・緊急時に停止可能な情報機器と業務継続のため無停止が求められる情報機器についても事前に把握しておく。

【参考】

・「政府機関等における情報システム運用継続計画ガイドライン」の改定について（NISC）
https://www.nisc.go.jp/policy/group/general/itbcp-guideline.html

④構成員へのセキュリティ意識の徹底

全構成員が主体的にサイバーセキュリティ等の確保に取り組むべきであることを認識するよう、意識づけを行う。

【例】

・全構成員に対する情報セキュリティ教育の受講
・新たに構成員になるものに対しての情報セキュリティ教育の実施

【参考】

・富山大学の構成員に対する情報セキュリティ教育の効果把握（JST 学術情報処理研究 22 巻（2018）1 号）
https://www.jstage.jst.go.jp/article/jacn/22/1/22_JACN22-1-9/_article/-char/ja/

４．サプライチェーンリスクへの対応

（１）外注や共同研究、重要プロジェクトにかかるリスク管理

外部委託や共同研究等の実施状況などを把握した上で、保有する情報のリスク度に応じた取り扱いが委託先や共同研究等参加機関でなされているか確認すること。

また、特にリスク評価が高い情報を取り扱う情報システムについて、サプライチェーンリスクに留意すること。

【例】

- 情報システム調達を情報システム部門およびセキュリティ部門、CSIRT 等で必ず確認する仕組みを構築する。
- 外部委託先において必要なセキュリティ対策が確実に実施されるよう、外部委託先に求めるセキュリティ要件を各大学等内で統一的に整備し、調達仕様書等へ記載するとともに、外部委託先における対策の履行状況を確認する。
- 情報システム・機器・役務・サービス（外部ホスティングサービスやクラウド等を利用している場合を含む）等の調達に当たっては、サプライチェーンリスクを軽減するための要求要件を調達仕様書に記載する。
- 共同研究など外部機関が保有する情報を管理する場合は、産業競争力強化法（平成二十五年法律第九十八号）第二条第十九項第一号の規定に基づき定められた「技術及びこれに関する研究開発の成果、生産方法その他の事業活動に有用な情報の漏えいを防止するために必要な措置に関する基準」も参考に対応を行う。

【参考】

- サプライチェーンのセキュリティ脅威に備える（IPA）
  https://www.ipa.go.jp/files/000073868.pdf

- IT 調達に係る国等の物品等又は役務の調達方針及び調達手続に関する申合せ（NISC）
  https://www.nisc.go.jp/pdf/policy/general/choutatsu_moushiawase0706.pdf

５．インシデント対応体制の構築

（１）インシデントの緊急体制と復旧体制の整備

サイバー攻撃による被害を受けた場合、被害原因の特定および解析を速やかに実施できるよう体制を構築する。

【例】

- 速やかな各種ログの保全や感染端末の確保等の証拠保全が行える体制を構築する
- 外部のセキュリティベンダなど関係機関との連携による調査が行えるよう指示する。
- インシデント発生時の所管省庁等への報告手順も含めて連絡体制を整えるとともに、演習を行う。
- インシデント発生後、再発防止策の検討にあたっては、必要に応じて外部の専門家の知見も活用することも検討する。
- 緊急連絡網（システム運用、セキュリティベンダなどの連絡先)、社外を含む情報開示の通知先一覧を整備し、対応に従事するメンバーに共有しておく。
- 初動対応時にはどのような業務影響が出るか検討し、緊急時に関係部署が速やかに協力できるよう予め取り決めをしておく。
- インシデントに関する被害状況、他社への影響等について経営者に報告する。

【参考】

- CSIRT マテリアル（一般社団法人 JPCERT コーディネーションセンター）
  https://www.jpcert.or.jp/csirt_material/?msclkid=9a73a76bc47b11ecaf3e514057849e71

６．セキュリティ運用の実施

（１）脅威動向や脆弱性情報取集、監視、侵入の特定などの運用について

世情を踏まえた脅威動向など、日次の脅威動向や脆弱性情報の収集の収集を行うこと。

【例】

- 機関内で利用している情報システム機器・ソフトウェアにかかる脆弱性情報を収集する。
- 脆弱性情報を自動で収集する仕組みを活用する。
- サイバー攻撃に痕跡にかかる技術情報、いわゆる IoC 情報についても収集し、自組織に対するセキュリティ攻撃への防御への活用に生かすこと。
- IoC 情報については継続的かつ迅速な更新が重要であるが、手動での更新は非常に煩雑であるため、ファイアウォールやウイルス対策ソフト等により危険なサイトや IP アドレス等へのアクセスをフィルタリング（ウェブフィルタや IP レピュテーションなど）を行う仕組みを活用する。

【参考】

- システム管理基準（平成 30 年 4 月 20 日改訂）(経済産業省)
  https://www.meti.go.jp/policy/netsecurity/sys-kansa/h30kaitei.html

- 情報セキュリティ管理基準 （平成 28 年改正版）(経済産業省)
  https://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Management_Standard_H28.pdf

７．監査等での運用チェック

（１）技術的、オペレーション等の監査について

年に一度、情報セキュリティ対策基本計画の進捗を確認し、フォローアップすること。

また、情報セキュリティ監査を定期的（毎年度）に実施し、脆弱性対応の確認、業務オペレーションの確認を行うこと。

【例】

- 情報セキュリティ監査の指摘事項に対する改善策を対策基本計画に反映し、継続的にフォローアップを行う。
- 中立性を担保するため、第三者による情報セキュリティ監査を実施する。
- 監査の実施内容として、情報システムの脆弱性診断だけでなく、情報セキュリティポリシーや実施手順書等の遵守状況を確認するために行うマネジメント監査についても実施する。

【参考】

- 情報セキュリティ監査実施手順の策定手引書（平成 29 年 4 月）（NISC）
  https://www.nisc.go.jp/pdf/policy/general/SecurityAuditManual.pdf

- システム監査基準（平成 30 年 4 月 20 日改訂）（経済産業省）
  https://www.meti.go.jp/policy/netsecurity/sys-kansa/h30kaitei.html